ABSTRACT

The present invention offers a prime calculating apparatus for achieving prime calculation where producing identical primes is avoided by simple management techniques. The prime calculating apparatus stores a known prime q and management information unique in the use range of primes. The prime calculating apparatus reads the management information; generates random information R based on the read management information; reads prime q; calculates prime candidate N, according to N = 2 × random information R × prime q + 1, using the read prime q and generated random information R; tests whether the calculated prime candidate N is a prime; and outputs the calculated prime candidate N as a prime when the primality of the calculated prime candidate N is determined. Herewith, the prime calculating apparatus is able to calculate prime candidates from unique management information while avoiding producing identical primes.